

FIGURE 10.8 Biometric devices provide high levels of computer and network security because they monitor human body characteristics that can't be stolen. IriScan's PC Iris (above) can compare the patterns in the iris of the user against a database of employees and other legitimate users. The U-Match Bio-Link Mouse (right) checks the thumbprint of the user against a database of prints approved for access.

2. Any computer can do only what it is programmed to do. "[I]t cannot protect itself from either malfunctions or deliberate attacks unless such events have been specifically anticipated, thought through, and countered with appropriate programming."

Computer owners and administrators use a variety of security techniques to protect their systems, ranging from everyday low-tech locks to high-tech software scrambling.

Physical Access Restrictions

One way to reduce the risk of security breaches is to identify people attempting to access computer equipment. Organizations use a number of tools and techniques to identify personnel. Computers can perform some security checks; human security guards perform others. Depending on the security system, you might be granted access to a computer based on the following criteria:

- *Something you have*, such as a key, an ID card with a photo, or a *smart card* containing digitally encoded identification in a built-in memory chip
- *Something you know*, such as a password, an ID number, a lock combination, or a piece of personal history, such as your mother's maiden name
- *Something you do*, such as your signature or your typing speed and error patterns
- *Something about you*, such as a voice print, fingerprint, retinal scan, facial feature scan, or other measurement of individual body characteristics; these measurements are collectively called **biometrics**.

Because most of these security controls can be compromised—keys can be stolen, signatures can be forged, and so on—many systems use a combination of controls. For example, an employee might be required to show a badge, unlock a door with a key, and type a password to use a secured computer.

In the days when corporate computers were isolated in basements, physical restrictions were sufficient for keeping out intruders. But in the modern office, computers and data are everywhere, and networks connect computers to the outside world. In a distributed, networked environment, security is much more problematic. It's not enough to restrict physical access to mainframes when personal computers and network connections aren't restricted.

Passwords and Access Privileges

Passwords are the most common tools used to restrict access to PCs, mainframe computers, and Web sites. Passwords are effective, however, only if they're chosen carefully. Most computer users choose passwords that are easy to guess: names of partners, or pets; words related to jobs or hobbies; and consecutive characters on keyboards. The most popular passwords include 123456, qwerty, abc123, letmein, monkey, myspace1, god, sex, money, love, and, of course, password. Hackers know and exploit these clichés; cautious users avoid them. They also use dictionary programs to guess passwords systematically by, in effect, trying every word in the dictionary. That's why many security systems refuse to let you choose a real word or name as a password. The best passwords mix letters and numbers into strings that make no sense to anyone except the people who use them. Even the best passwords should be changed frequently.

Access-control software doesn't need to treat all users identically. Many systems use passwords to restrict users so they can open only files related to their work. In many cases, users are given read-only access to files that they can see but not change.

Even a PC can have different levels of access, because Windows, Mac OS X, and Linux all support multiple users. When a PC is set up with multiple user accounts, each user has a unique user ID and password. When one of those users logs into the PC with his user ID and password, he has access only to his own personal files plus any shared files that are accessible to multiple users. When he logs out, another user can log in to the same PC and use a completely different set of files. (A PC or Mac can easily be set up to bypass the login screen and automatically open a single user's account without a password.)

At least one of the accounts on a PC or Mac must be a **system administrator** account. The administrator has additional access privileges—permission to install software applications, change system settings, and more. Users who don't have administrator-level access are denied access to many of the “under the hood” components of the system.

Web sites frequently use passwords as access keys. Enterprising criminals often use software bots to sign up automatically for accounts and passwords. To foil the bots, many sites use answer-back security systems. When you apply for membership in such a system, you might be required to give your email address. The system sends an email to you and you reply, ensuring that you're a real person with a real email address.

Bots are also used to log into sites with stolen or guessed passwords. Many sites require passwords and visual identification of a string of abstract characters—something that's easy for a person to identify, but not easy for a machine to read.

Firewalls, Encryption, and Audits

Many data thieves do their work without breaking into computer systems; instead, they intercept messages as they travel between computers on networks. Passwords are of little use for hiding email messages when they're traveling through Internet cables or wireless connections. Many organizations use **firewalls** to keep their internal networks secure while enabling communication with the rest of the Internet. The technical details of firewalls vary considerably, but they're all designed to serve the same function: to guard against unauthorized access to an internal network. In effect, a firewall is a gate with a lock; the locked gate opens only for information packets that pass one or more security inspections. Firewalls aren't just for large corporations. Without firewall hardware or software installed, a home computer with an always-on DSL or cable modem connection can be easy prey for Internet snoopers. Windows Vista and Mac



FIGURE 10.9 Hardware firewall products come in all shapes and sizes.

How It Works

10.1 Firewalls

A firewall is a program, often run on a dedicated computer, that filters information between a private network and the rest of the Internet. A set of security rules, created by a network administrator, determines which packets can enter and leave the local network.

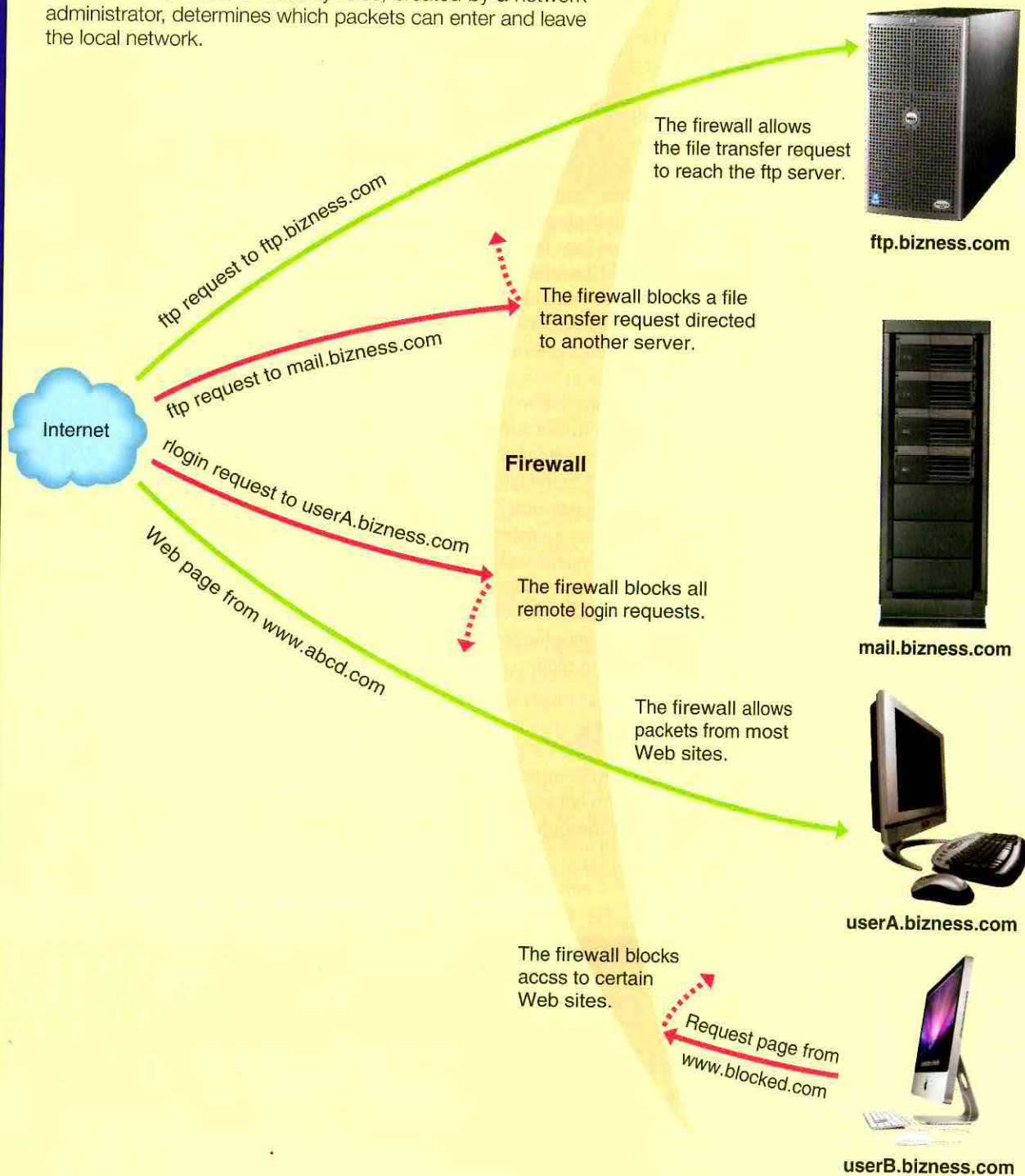


FIGURE 10.10

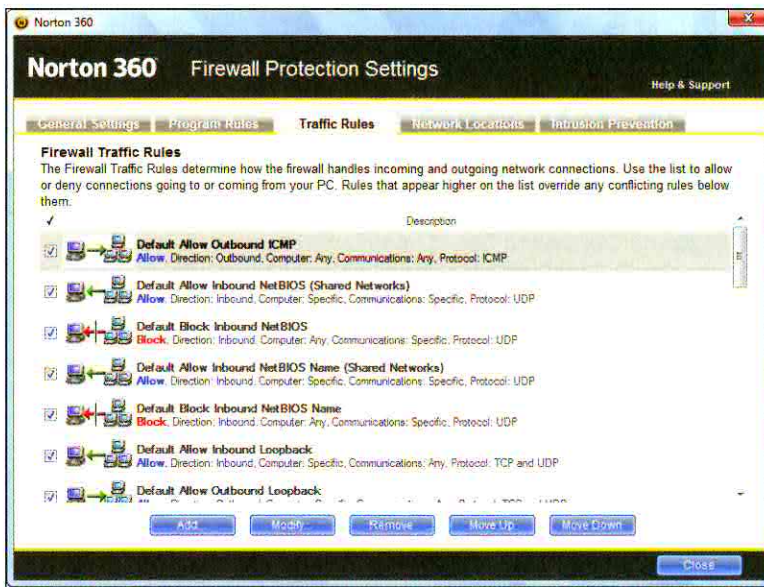


FIGURE 10.11 Software firewalls, such as the one included with Norton 360, help protect home networks from hackers.

OS X include basic software firewalls, but these firewalls must be activated before they can provide protection.

Of course, the firewall's digital drawbridge has to let some messages pass through; otherwise there could be no communication with the rest of the Internet. How can those messages be secured in transit? To protect transmitted information, many organizations and individuals use **encryption** software to scramble their transmissions. When a user encrypts a message by applying a secret numerical code, called an **encryption key**, the message can be transmitted or stored as an indecipherable garble of characters. The message can be read only after it's been reconstructed with a matching key.



FIGURE 10.12 The encryption process.

How It Works

10.2 Cryptography

If you want to be sure that an email message can be read by only the intended recipient, you must either use a secure communication channel or secure the message.

Mail within many organizations is sent over secure communication channels—channels that can't be accessed by outsiders. But you can't secure the channels used by the Internet and other worldwide mail networks; there's no way to shield messages sent through public telephone lines and airwaves. In the words of Mark Rotenberg, director of the Electronic Privacy Information Center, "Email is more like a postcard than a sealed letter."

If you can't secure the communication channel, the alternative is to secure the message. You secure a message by using a cryptosystem to encrypt it—scramble it so it can be decrypted (unscrambled) only by the intended recipient.

Almost all cryptosystems depend on a key—a passwordlike number or phrase that can be used to encrypt or decrypt a message. Eavesdroppers who don't know the key have to try to decrypt it by brute force by trying all possible keys until they guess the right one.

Some cryptosystems afford only modest security: A message can be broken after only a day or week of brute force cryptanalysis on a supercomputer. More effective systems would take a supercomputer billions of years to break the message.

The traditional kind of cryptosystem used on computer networks is called a symmetric secret key system. With this approach the sender and recipient use the same key, and they have to keep the shared key secret from everyone else.

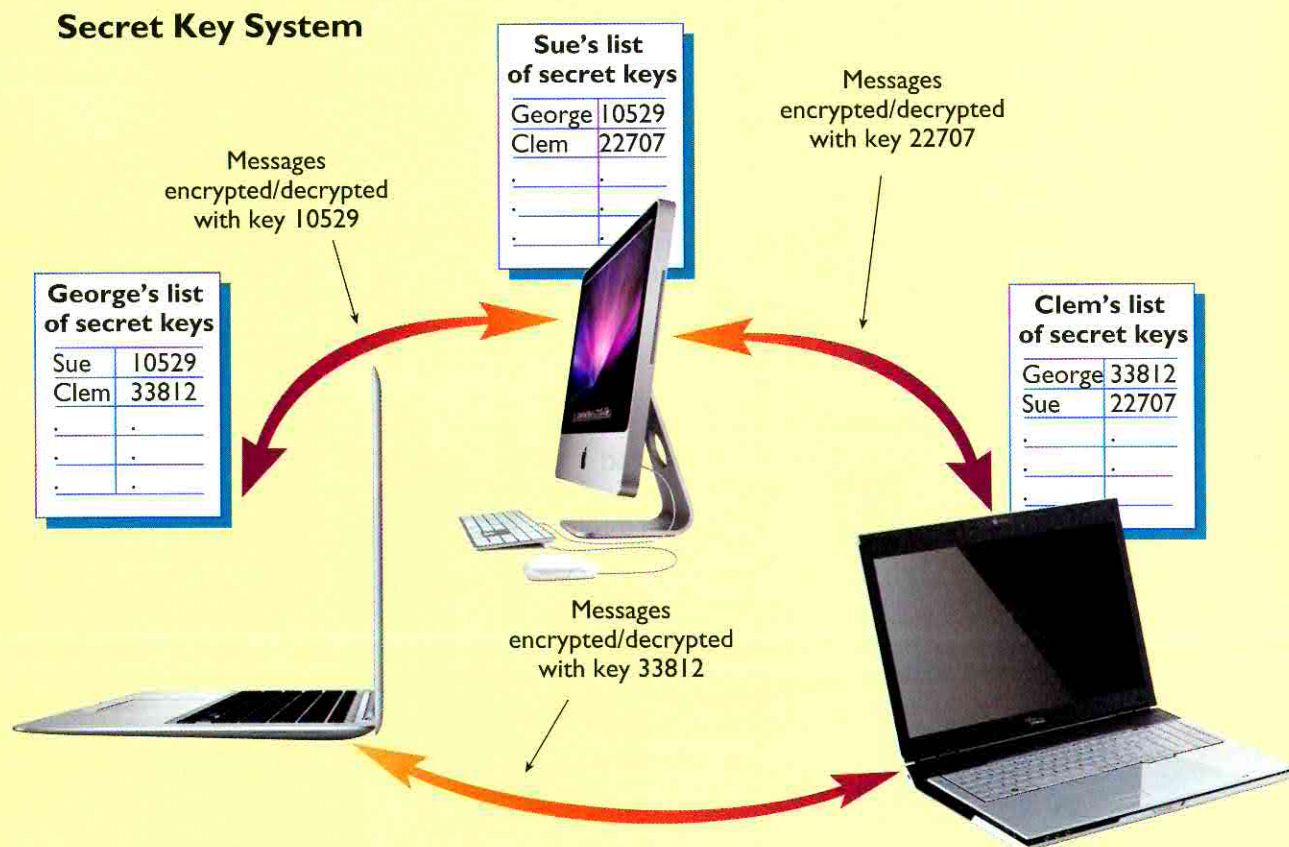
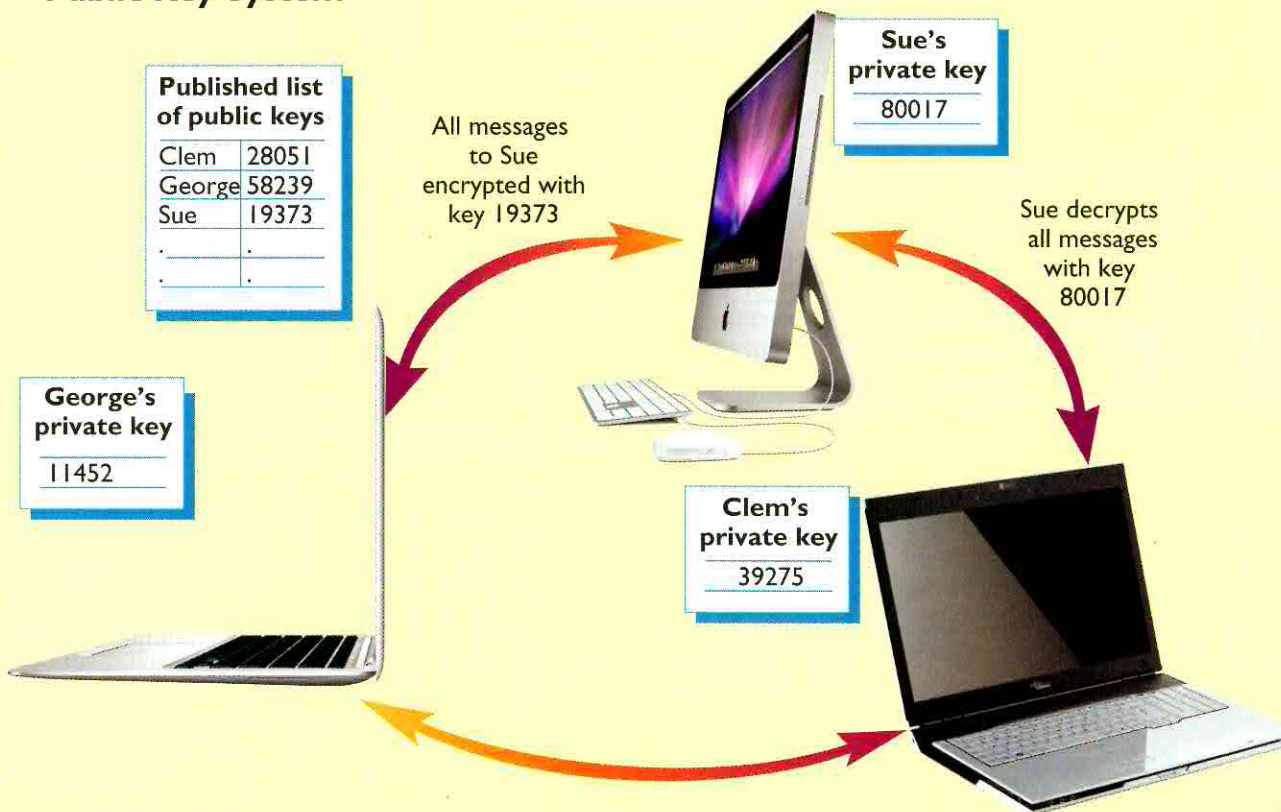


FIGURE 10.13

The biggest problem with symmetric secret key systems is key management. If you want to communicate with several people and ensure that each person can't read messages intended for the others, then you'll need a different secret key for each person. When you want to communicate with new people, you have the problem of letting them know what the key is. If you send it over the ordinary communication channel, it can be intercepted.

In the 1970s cryptographers developed public key cryptography to get around the key management problems. The most popular kind of public key cryptosystem, RSA, is being incorporated into most new network-enabled software. Phillip Zimmerman's popular shareware utility called PGP (for Pretty Good Privacy) uses RSA technology.

Public Key System



Each person using a public key cryptosystem has two keys: a private key known only to the user and a public key that is freely available to anyone who wants it. Thus a public key system is asymmetric: A different key is used to encrypt than to decrypt. Public keys can be published in phone directories, Web pages, and advertisements; some users include them in their email signatures.

If you want to send a secure message over the Internet to your friend Sue in St. Louis, you use her public key to encrypt the message. Sue's public key can't decrypt the message; only her private key can do that. The private key is specifically designed to decrypt messages that were encrypted with the corresponding public key. Because public/private key pairs can be generated by individual users, the key distribution problem is solved. The only keys being sent over an insecure network are publicly available keys.

You can use the same technology in reverse (encrypt with the private key, decrypt with the public key) for message authentication: When you decrypt a message, you can be sure that it was sent from a particular person on the network. In the future, legal and commercial documents will routinely have digital signatures that will be as valid as handwritten ones.

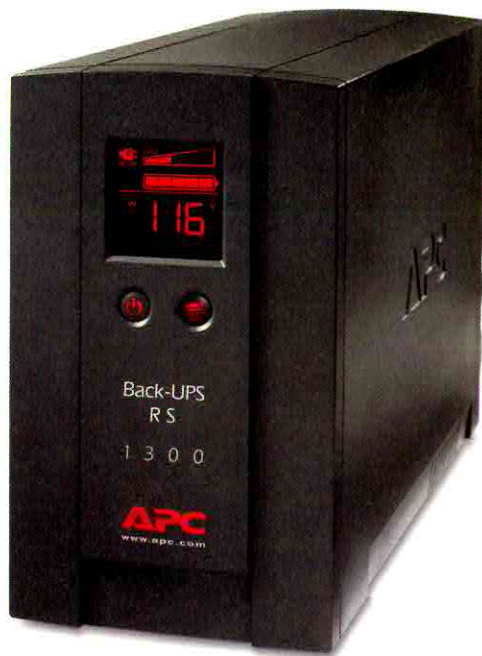


FIGURE 10.14 An uninterruptible power supply (UPS) protects a computer against power surges and momentary power loss.



FIGURE 10.15 A RAID storage device combines hard drives to create a redundant data store that can withstand hardware failures.

For the most sensitive information, passwords, firewalls, and encryption aren't enough. A diligent spy can "listen to" and possibly read compromising emanations (CE)—the electromagnetic signals that emanate from computer hardware and, in some cases, read sensitive information. To prevent spies from using these spurious broadcasts, the NSA has invested heavily in TEMPEST, a program to secure electronic communication from eavesdroppers while enabling the U.S. government to intercept and interpret those signals from other sources.

Audit-control software is used to monitor and record computer transactions as they happen so auditors can trace and identify suspicious computer activity after the fact. Effective audit-control software forces every user, legitimate or otherwise, to leave a trail of electronic footprints. Of course, this kind of software is of little value unless someone in the organization monitors and interprets the output.

Backups and Other Precautions

Even the tightest security system can't guarantee absolute protection of data. A power surge or a power failure can wipe out the most carefully guarded data in an instant. An **uninterruptible power supply (UPS)** can protect computers from data loss during power failures; inexpensive ones can protect home computers from short power dropouts. *Surge protectors* don't help during power failures, but they can shield electronic equipment from dangerous power spikes, preventing expensive hardware failures.

Of course, disasters come in many forms. Sabotage, human errors, machine failures, fire, flood, lightning, and earthquakes can damage or destroy computer data along with hardware. Any complete security system should include a plan for recovering from disasters. For mainframes and PCs alike, the best and most widely used data recovery insurance is a system of making regular **backups**. For many systems, data and software are backed up automatically onto disks or tapes, usually at the end of each workday. Most data processing shops keep several **generations** of backups so they can, if necessary, go back several days, weeks, or years to reconstruct data files. Storage technology called **RAID (redundant array of independent disks)** enables multiple hard disks to operate as a single logical unit. RAID systems can, among other things, automatically *mirror* data on multiple disks, effectively creating instant redundancy.

For maximum security, many computer users keep copies of sensitive data off-site—in one or more remote locations. Off-site backups minimize the chances that fires, floods, or other local disasters will completely destroy important data. One type of off-site backup that's rapidly growing in popularity is online backup. Many companies, including Internet service providers, Web hosting companies, and security software companies, offer online storage for their customers to use for backing up data. Some of these sites provide special software for backing up data; others can be used with any backup software. Of course, backup speed is limited by connection bandwidth, and is typically much slower than backing up to a local hard disk.

Human Security Controls

Security experts throughout the computer industry are constantly developing new technologies and techniques for protecting computer systems from computer criminals. At the same time, criminals continue to refine their craft. In the ongoing competition between the law and the lawless, computer security generally lags behind. In the words of Tom Forester and Perry Morrison in *Computer Ethics*, "Computer security experts are forever trying to shut the stable door after the horse has bolted." Ultimately, computer security is a human problem that can't be solved by technology alone.